

EXHIBIT 1 TO EXHIBIT A

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

CYBERFONE SYSTEMS, LLC,

Plaintiff,

v.

AMAZON.COM INC., *et al.*,

Defendants.

C.A. No. 11-831-SLR

PROTOCOL FOR PRODUCTION OF ESI

1. Scope

a. The provisions set forth herein shall govern the production of electronically stored information (ESI) between the parties.

2. General Provisions

a. **Preservation of Discoverable Information.** A party shall take reasonable and proportional steps to preserve discoverable information in the party's possession, custody or control.

(i) Absent a showing of good cause by the requesting party, the parties shall not be required to modify, on a going-forward basis, the procedures used by them in the ordinary course of business to back up and archive data; provided, however, that the parties shall preserve the non-duplicative discoverable information currently in their possession, custody or control.

(ii) Absent a showing of good cause by the requesting party, the categories of ESI identified in Schedule A attached hereto need not be preserved or restored.

(iii) No party need employ forensic data collection or tracking methods and technologies, but instead may make electronic copies for collection and processing purposes using widely-accepted methods, except when and to the extent there is good cause to believe specific, material concerns about authenticity or spoliation exist with respect to specific documents and materials. If a receiving party believes that there is such good cause, then the producing party and the receiving party shall meet and confer in good faith to determine the extent to which forensic and other data associated with the specific documents and materials should be produced.

b. Privilege.

(i) The parties are to confer on the nature and scope of privilege logs for the case, including whether categories of information may be excluded from any logging requirements and whether alternatives to document-by-document logs can be exchanged.

(ii) With respect to information generated after the filing of the complaint, parties are not required to include any such information in privilege logs.

(iii) Activities undertaken in compliance with the duty to preserve information are protected from disclosure and discovery under Fed. R. Civ. P. 26(b)(3)(A) and (B).

(iv) The parties agree that pursuant to Federal Rule of Evidence 502(d), the inadvertent production of a privileged or work product protected document or email is not a waiver in the actions or in any other federal or state proceeding. Further, the mere production of documents and emails in the actions, as a part of a mass production, shall not itself constitute a waiver for any purpose.

(v) The parties believe it is necessary to apply to the Court for a protective order specifying the terms and conditions for the disclosure of confidential information and have submitted a proposed protective order for the Court's consideration contemporaneously herewith.

3. **Initial Discovery Conference.**

a. **Timing.** Consistent with the guidelines that follow, the parties shall discuss the parameters of their anticipated discovery at the initial discovery conference (the "Initial Discovery Conference") pursuant to Fed. R. Civ. P. 26(f), which shall take place before the Fed. R. Civ. P. 16 scheduling conference ("Rule 16 Conference").

b. **Content.** The parties shall discuss the following:

(i) The issues, claims and defenses asserted in the case that define the scope of discovery.

(ii) The likely sources of potentially relevant information (*i.e.*, the "discoverable information"), including witnesses, custodians and other data sources (*e.g.*, paper files, email, databases, servers, etc.).

(iii) Technical information, including the exchange of production formats.

(iv) The existence and handling of privilege information.

(v) The categories of ESI that should be preserved.

4. **Initial Disclosures.** Within 30 days after the Rule 16 Conference, each party shall disclose:

a. **Custodians.** The 10 custodians most likely to have discoverable information in their possession, custody or control. The custodians shall be identified by name, title, role in the instant dispute, and the subject matter of the information.

b. **Non-custodial data sources.**¹ A list of the non-custodial data sources that are most likely to contain non-duplicative discoverable information for preservation and production consideration.

c. **Notice.** The parties shall identify any issues relating to:

(i) Any ESI (by type, date, custodian, electronic system or other criteria) that a party asserts is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(C)(i).

(ii) Third-party discovery under Fed. R. Civ. P. 45 and otherwise, including the timing and sequencing of such discovery.

(iii) Production of information subject to privacy protections, including information that may need to be produced from outside of the United States and subject to foreign laws.

5. Specific E-Discovery Issues.

a. **On-site inspection of electronic media.** Such an inspection shall not be permitted absent a demonstration by the requesting party of specific need and good cause.

b. **Search methodology.** The producing party shall search (i) the non-custodial data sources identified in accordance with paragraph 4(b); (ii) other ESI maintained by the

¹ That is, a system or container that stores ESI, but over which an individual custodian does not organize, manage or maintain the ESI in the system or container (*e.g.*, enterprise system or database).

custodians identified in accordance with paragraph 4(a); and (iii) emails in accordance with paragraph 6.

c. **Temporal scope.** ESI and non-ESI shall be limited to a term of six (6) years preceding the date the original Complaint was filed, except that discovery with regard to (i) conception, development, reduction to practice commercialization, licensing and prosecution of the Patents-in-Suit and prior art; and (ii) notice of the Patents-in-Suit, licenses for similar technology by the defendants and defendants' patent applications (including parent applications) for similar technology, if any, are not so limited.

d. **Cost Shifting.** Costs will be shifted for disproportionate ESI, non-ESI and email production requests pursuant to Federal Rule of Civil Procedure 26. Likewise, a party's nonresponsive or dilatory discovery tactics will be cost-shifting considerations.

e. **Format.** ESI and non-ESI shall be produced to the requesting party as black and white text searchable image files (*e.g.*, PDF or TIFF). When a text-searchable image file is produced, the producing party must preserve the integrity of the underlying ESI, *i.e.*, the original formatting, the metadata (as noted below) and, where applicable, the revision history. The parties shall produce their information in the following format: single page TIFF images and associated multi-page text files containing extracted text or OCR with Concordance and Opticon load files containing all requisite information including relevant metadata and to indicate the location and unitization of TIFF files. A document that cannot be processed shall be represented in the production set with a slip-sheet indicating that the document was not processed or it shall be listed on an electronic exception report in a spreadsheet or similar format.

f. **Document Unitization.** If a document is more than one page, the unitization of the document and any attachments and/or affixed notes shall be maintained as they existed in the original document. That unitization shall be reflected in the load file described above. For email attachments, appropriate attachment fields in the load file shall accompany the beginning and ending production numbers for the email.

g. **Color.** If the need arises to view a particular document or email in color, a party can make a good faith request to receive color images for that document. No images, including JPEG images, shall be compressed using the LZW (Lempel-Ziv & Welch) algorithm.

h. **Native files.** The only files that should be produced in native format are files not easily converted to image format, such as Excel and Access files, or files for which conversion to image format is impracticable or unreasonable (such as video or audio files).

i. **Metadata fields.** The parties shall meet and confer to discuss whether the production of metadata is appropriate. Only after such a meet and confer will the parties be obligated to produce metadata, if at all. Further, in no event will either party be required to produce metadata, to the extent such metadata exists, other than the following: Custodian, Email Subject, From, To, CC, BCC, Date Sent, Time Sent, Date Received, Time Received, Filename, Author, Date Created, Attachment Begin, and Attachment End (or the equivalent thereof).

6. Discovery of Emails

a. General ESI production requests under Federal Rules of Civil Procedure 34 and 45 shall not include email. To obtain email, parties must propound specific email production requests.

b. Email production requests shall only be propounded for specific issues, rather than general discovery of a product or business. Further, email production requests will only apply to emails actually sent or received and will not seek the production of “draft” emails.

c. Discovery of emails shall be phased to occur after the parties have met and conferred in good faith to discuss the scope and procedure for email discovery, which shall occur only during the damages phase of the case and will be limited to issues relating to damages.

d. Email production requests shall specifically identify the custodian, search terms, and time frame requested.

e. Subject to the foregoing limitations, a requesting party shall not serve email production requests seeking emails from more than five custodians per producing party for all such requests. The parties may jointly agree to modify this limit without the Court’s leave. The Court shall consider contested requests for up to five additional custodians per producing party, upon showing a distinct need based on the size, complexity, and issues of this specific case. Should a party serve email production requests for additional custodians beyond the limits agreed to by the parties or granted by the Court pursuant to this paragraph, the requesting party shall bear all reasonable costs associated with these discovery requests.

f. Subject to the foregoing limitations, each requesting party shall limit its email production requests to a total of five search terms per custodian per party. The parties may jointly agree to modify this limit without the Court's leave. The Court shall consider contested requests for up to five additional search terms per custodian, upon showing a distinct need based on the size, complexity, and issues of this specific case. The search terms shall be narrowly tailored to particular issues. Indiscriminate terms, such as the producing company's name or its product name, are inappropriate unless combined with narrowing search criteria that sufficiently reduce the risk of overproduction. A conjunctive combination of multiple words or phrases (*e.g.*, "computer" and "system") narrows the search and shall count as a single search term. A disjunctive combination of multiple words or phrases (*e.g.*, "computer" or "system") broadens the search, and thus each word or phrase shall count as a separate search term unless they are variants of the same word. Use of narrowing search criteria (*e.g.*, "and," "but not," "w/x") is encouraged to limit the production and shall be considered when determining whether to shift costs for disproportionate discovery. Should a party serve Email production requests with search terms beyond the limits agreed to by the parties or granted by the Court pursuant to this paragraph, the requesting party shall bear all reasonable costs associated with these discovery requests.

g. Discovery of emails shall be limited to a term of six (6) years from the date of the filing of the first Complaint.

7. Production of Source Code

a. The parties agree that, to the extent source code is made available for inspection, it will be made available pursuant to a mutually agreeable protective order to be entered in this case.

b. The parties agree that non-text (*i.e.*, non readable) source code files, including, but not limited to, binary executable files, object code files, compilers and linkers, do not need to be produced.

SCHEDULE A

1. Deleted, slack, fragmented, disaster recovery media or other data only accessible by forensics.
2. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.
3. On-line access data such as temporary internet files, history, cache, cookies, and the like.
4. Data in metadata fields that are frequently updated automatically, such as last-opened dates.
5. Back-up data that are substantially duplicative of data that are more accessible elsewhere.
6. Voice messages.
7. Instant messages that are not ordinarily printed or maintained in a server dedicated to instant messaging.
8. Electronic mail or pin-to-pin messages sent to or from mobile devices (e.g., iPhone and Blackberry devices), cell phone texts, or messages posted on any social media sites (e.g., Facebook or Twitter).
9. Other electronic data stored on a mobile device, such as calendar or contact data or notes.
10. Logs of calls made from mobile devices.
11. Server, system or network logs.

12. Electronic data temporarily stored by laboratory equipment or attached electronic equipment, provided that such data is not ordinarily preserved as a part of a laboratory report.

13. Data remaining from systems no longer in use that is unintelligible on the systems in use.